

**UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF GEORGIA
SAVANNAH DEVISION**

LANA CLARK, on behalf of herself and all
others similarly situated,

Plaintiff,

v.

TMX FINANCE CORPORATE SERVICES,
INC.,

Defendant.

Case No.: CV423-168

CLASS ACTION COMPLAINT

DEMAND FOR JURY TRIAL

Plaintiff Lana Clark (“Plaintiff”), individually and on behalf of all others similarly situated, brings this Class Action Complaint against TMX Finance Corporate Services, Inc. (“Defendant” or “TMX”), and alleges as follows:

I. INTRODUCTION

1. This action stems from TMX’s failure to secure the sensitive personal information of more than 4.8 million of its customers. TMX provides consumer credit products under the TitleMax®, TitleBucks®, and InstaLoan® brands.¹ Through each of these brands, TMX obtains certain personally identifying information of its customers—current and former loan borrowers, as well as loan applicants—in furtherance of services it performs on their behalf.

2. TMX failed to properly secure and safeguard sensitive Personally Identifiable Information provided by and belonging to its customers, including (without limitation) name, date of birth, passport number, driver’s license number, federal/state identification card number, tax identification number, Social Security number and/or financial account information, and

¹ <https://www.tmxfinancefamily.com/what-we-do/>.

other information such as phone number, address, and email address (“PII”).

3. On or around March 30, 2023, Defendant notified potentially impacted customers of the Data Breach, stating that, “On February 13, 2023, we detected suspicious activity on our systems and promptly took steps to investigate the incident. As part of that investigation, global forensic cybersecurity experts were retained. Based on the investigation to date, the earliest known breach of TMX’s systems started in early December 2022. On March 1, 2023, the investigation confirmed that information may have been acquired between February 3, 2023 – February 14, 2023” (the “Data Breach”).

4. At least 4.8 million individuals were affected by the Data Breach.

5. By obtaining, collecting, using, and deriving a benefit from Plaintiff’s and Class Members’ PII, Defendant owed these individuals a duty to take all reasonable and necessary measures to keep it safe and secure from unauthorized access. Defendant admits that the PII accessed and potentially exfiltrated in the hacking incident includes personal information, including the forms of PII referenced in paragraph 2 above.

6. The exposed PII of Defendant’s current and former customers can be sold on the dark web, a black market for such information. Hackers can now access and/or offer the PII for sale to criminals for improper use. As a result of the Data Breach, Defendant’s current and former customers face a lifetime risk of identity theft—a present and indefinite threat heightened by the loss of their Social Security numbers.

7. Until notified of the Data Breach, Plaintiff and Class Members had no idea their PII had been compromised, subjecting them to a significant risk of identity theft and various other types of personal, social, and financial harm.

8. Plaintiff brings this action on behalf of all persons whose PII was compromised in

the Data Breach as a result of Defendant's failure to: (i) adequately protect the PII of its current and former customers; (ii) warn its current and former customers of its inadequate information security practices; and (iii) effectively secure hardware containing protected PII using reasonable and effective security procedures free of vulnerabilities. Defendant's conduct constitutes negligence, an egregious privacy invasion, and a violation of statutory law.

9. Plaintiff and Class Members have suffered actual and imminent injuries as a direct result of the Data Breach, including: (a) theft of their PII; (b) costs associated with the detection and prevention of identity theft; (c) costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the consequences of this breach; (d) invasion of privacy; (e) the emotional distress, stress, nuisance, and annoyance of responding to, and resulting from, the Data Breach; (f) the actual and/or imminent injury arising from actual and/or potential fraud and identity theft resulting from their personal data being placed in the hands of the ill-intentioned hackers and/or criminals; (g) damage to and diminution in value of their personal data entrusted to Defendant with the mutual understanding that Defendant would safeguard their PII against theft and not allow access to and misuse of their personal data by any unauthorized third party; and (h) the continued risk to their PII, which remains in the possession of Defendant, and which is subject to further injurious breaches so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' PII.

10. Defendant states it will protect the privacy of its customers and maintain security measures to protect its customers' information from unauthorized disclosure.² Nevertheless,

² <https://www.tmxdisclosures.com/titlemax/privacy-policy>;
<https://www.tmxdisclosures.com/instaloan/privacy-policy>;
<https://www.tmxdisclosures.com/titlebucks/privacy-policy>.

Defendant, in reckless disregard of the rights of Plaintiff and Class Members, failed to adopt and implement adequate and reasonable measures to ensure that Defendant's current and former customers' PII was safeguarded and failed to take available steps to prevent an unauthorized disclosure of data. In consequence, the PII of Plaintiff and Class Members was compromised and exfiltrated by an unknown and unauthorized third party. Plaintiff and Class Members have a strong continuing interest in ensuring that their information is and remains safe and secure.

11. Accordingly, Plaintiff by this action seeks compensatory damages together with injunctive relief to remediate TMX's failure to secure her and other Class Members' PII, and requiring TMX to provide credit monitoring, identity theft insurance, and credit repair services to protect the Class of Data Breach victims from identity theft and fraud.

II. PARTIES

Plaintiff Lana Clark

12. Plaintiff Lana Clark is a resident and citizen of the State of California.

Defendant TMX Finance Corporate Services, Inc.

13. Defendant TMX Finance Corporate Services, Inc. ("TMX") provides consumer credit products to its customers. TMX is organized under the laws of Georgia with its principal place of business at 15 Bull Street, Suite 200, Savannah, GA 31401.

14. All of Plaintiff's claims stated herein are asserted against Defendant and any of its owners, predecessors, successors, subsidiaries, agents and/or assigns.

III. JURISDICTION AND VENUE

15. This Court has jurisdiction under 28 U.S.C. § 1332(d)(2) because this is a class action involving more than 100 Class Members and because the amount in controversy exceeds

\$5,000,000, exclusive of interest and costs. In addition, Plaintiff, numerous other Class Members, and Defendant are citizens of different states.

16. The Court has general personal jurisdiction over Defendant because, personally or through its agents, Defendant operated, conducted, engaged in, or carried on a business or business venture in Georgia; had offices in Georgia; and committed tortious acts in Georgia. As alleged above, Defendant is organized under the laws of Georgia and maintains its principal place of business in Savannah, Georgia.

17. Venue is proper in this District under 28 U.S.C. §§ 1391(a)(1), 1391(b)(1), 1391(b)(2), and 1391(c)(2). A substantial part of the events giving rise to the claims emanated from activities within this District, and Defendant resides, is headquartered and conducts substantial business in this District.

18. TMX's Terms of Use also state that, "any dispute arising under this Agreement shall be resolved exclusively by the state and federal courts of the State of Georgia, Chatham County and/or the City of Savannah."³

IV. FACTUAL ALLEGATIONS

Background

19. Defendant operates a "family of companies" to provide consumer credit products to consumers. This "family of companies" is comprised of TitleMax®, TitleBucks®, and InstaLoan®.

20. TitleMax is "one of the nation's largest title lending companies."⁴ On its website, TitleMax states that, "Every day, TitleMax helps thousands of people get the cash they need with a title loan, title pawn or now in select states, with a personal loan Since the first store's

³ <https://www.tmxdisclosures.com/tmx-finance-family/terms-of-use-privacy>.

⁴ <https://www.titlemax.com/about-us/>.

opening in 1998 in Georgia, TitleMax has expanded to over 900 locations spanning 14 states. With more than 2,000 team members nationwide, we pride ourselves on providing customers with clarity and confidence. You'll rest easy knowing that TitleMax is here to help.”⁵

21. TitleBucks is “one of America’s largest consumer lending companies.”⁶ TitleBucks has “helped hundreds of thousands of people with getting the cash they need.” TitleBucks’ website states that, “[t]here are now 60 conveniently located TitleBucks stores spanning six states. TitleBucks focuses on providing an exceptional level of customer service while also making the vehicle title-secured loan/pawn and personal loan process as quick and simple as possible.”⁷

22. InstaLoan is a loan provider which focuses on “providing people with the cash they need through the consumer loan that makes the most sense” whether it be a “1st lien loan, a signature loan, or a personal loan.”⁸ InstaLoan has 25+ locations, and its website states that “InstaLoan makes getting cash easy with our quick and convenient loan approval process.”⁹

23. Plaintiff and Class Members, who sought loan services from Defendant and/or its subsidiaries, were required to entrust Defendant with some of their most sensitive and confidential information, including, without limitation: name, date of birth, passport number, driver’s license number, federal/state identification card number, tax identification number, Social Security number and/or financial account information, and other information such as phone number, address, and email address. Certain of the information that Plaintiff entrusted to Defendant and/or its subsidiaries is effectively unchangeable and can be used to commit myriad

⁵ <https://www.titlemax.com/about-us/>.

⁶ <https://www.titlebucks.com/about-us/>.

⁷ <https://www.titlebucks.com/about-us/>.

⁸ <https://www.instaloan.com/about-us/>.

⁹ <https://www.instaloan.com/how-it-works/>.

financial crimes.

24. In providing services to Plaintiff and Class Members, Defendant and/or its subsidiaries retained sensitive personal information about Plaintiff and Class Members, including information concerning Defendant's loan services.

25. Plaintiff and Class Members, as current and former customers of Defendant, relied on Defendant to keep their PII confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information. Defendant's current and former customers require security to safeguard their PII.

26. Defendant operated under a continuous duty to adopt reasonable measures to protect Plaintiff's and Class Members' PII from involuntary disclosure to a third party.

The Data Breach

27. Defendant has posted Privacy Policies on its subsidiaries' websites.¹⁰ These Privacy Policies state that, "To protect your personal information from unauthorized access and use, we use security measures that comply with federal law. These measures include computer and mobile application safeguards and secured files and buildings. We also maintain physical, electronic and procedural safeguards (i.e., computer virus protection software, firewalls, encryption). Only authorized employees have access. Customer access to electronically stored account documents and information is protected via customer-created or customer-specific usernames and passwords."¹¹

¹⁰ <https://www.tmxdisclosures.com/titlemax/privacy-policy>;
<https://www.tmxdisclosures.com/titlebucks/privacy-policy>;
<https://www.tmxdisclosures.com/instaloan/privacy-policy>.

¹¹ *See id.*

28. The Privacy Policy also provides a list of instances in which disclosure of PII could be made to its affiliates and other entities without prior written authorization—none of which is applicable here.¹²

29. In or around early December, 2022, an intruder gained unauthorized access to the TMX network.¹³ TMX did not begin its investigation of this intrusion until February 13, 2023. It confirmed the breach on March 1, 2023.¹⁴ Between February 3 and February 14, 2023, an intruder accessed and exfiltrated the PII of over 4.8 million customers.¹⁵

30. On or around March 30, 2023, Defendant reported the Data Breach to state attorneys general offices, including those of Maine and California.¹⁶ At around the same time, Defendant also began notifying Plaintiff and Class Members of the Data Breach.¹⁷

31. On or around March 30, 2023, Defendant sent Plaintiff and Class members a form “Notice of Data Breach” detailing its findings. A sample of this letter is also posted on the Maine and California Attorneys General websites.¹⁸

32. The sample letter states in part:

TMX Finance Corporate Services, Inc., on behalf of itself, its parent TMX Finance LLC and its affiliates, many of which operate under the brands “TitleMax,” “TitleBucks,” and “InstaLoan” (collectively, “TMX”), is writing to inform you of a data breach that may have involved your personal information. TMX takes the

¹² *See id.*

¹³ <https://s3.documentcloud.org/documents/23735720/tmx-finance-sample-copy-of-individual-notice-l01.pdf>.

¹⁴ *Id.*

¹⁵ *See id.*; <https://apps.web.maine.gov/online/aeviewer/ME/40/179ab0ce-2c43-4119-ae5a-db766d4be3e0.shtml>.

¹⁶ <https://apps.web.maine.gov/online/aeviewer/ME/40/179ab0ce-2c43-4119-ae5a-db766d4be3e0.shtml>; <https://oag.ca.gov/ecrime/databreach/reports/sb24-564929>.

¹⁷ <https://s3.documentcloud.org/documents/23735720/tmx-finance-sample-copy-of-individual-notice-l01.pdf>.

¹⁸ *See id.*; <https://apps.web.maine.gov/online/aeviewer/ME/40/179ab0ce-2c43-4119-ae5a-db766d4be3e0.shtml>; <https://oag.ca.gov/ecrime/databreach/reports/sb24-564929>.

privacy and security of your personal information very seriously. This letter provides information about the incident and resources available to help you protect your information.

What Happened?

On February 13, 2023, we detected suspicious activity on our systems and promptly took steps to investigate the incident. As part of that investigation, global forensic cybersecurity experts were retained. Based on the investigation to date, the earliest known breach of TMX's systems started in early December 2022. On March 1, 2023, the investigation confirmed that information may have been acquired between February 3, 2023 – February 14, 2023. We promptly began a review of potentially affected files to determine what information may have been involved in this incident. We notified the FBI but have not delayed this notification for any law enforcement investigation.

What Information Was Involved?

The personal information involved may have included your name, date of birth, passport number, driver's license number, federal/state identification card number, tax identification number, social security number and/or financial account information, and other information such as phone number, address, and email address.

What We Are Doing.

Our investigation is still in progress, but TMX believes the incident has been contained. We continue to monitor our systems for any suspicious activity. We have implemented additional security features, such as additional endpoint protection and monitoring, as well as resetting all employee passwords. We continue to evaluate ways to further enhance the security of our systems. To help protect your identity, we are offering you complimentary credit monitoring and identity protection services through Experian IdentityWorksSM for a period of 12 months. Please see the enclosed Reference Guide for enrollment details and instructions on how to enroll.¹⁹

33. Defendant admits that unauthorized third persons accessed from its network

¹⁹ <https://s3.documentcloud.org/documents/23735720/tmx-finance-sample-copy-of-individual-notice-l01.pdf>.

systems sensitive information about current and former customers of Defendant.

34. Plaintiff's and Class Members' information can now be leaked onto the dark web, and/or may simply fall into the hands of companies that will use the detailed PII for targeted marketing without the approval of the affected current and former customers. In short, unauthorized individuals can readily access the PII of Defendant's current and former customers now that it has been stolen.

35. Defendant did not use reasonable security procedures and practices suitable or adequate to protect the sensitive information it was maintaining for current and former customers, causing the access and/or exfiltration of the PII of more than 4.8 million individuals.

Defendant Acquires, Collects and Stores Plaintiff's and Class Members' PII.

36. Defendant acquired, collected, and stored the PII of its current and former customers.

37. As a condition of doing business with Defendant, Defendant requires that its customers entrust Defendant with highly confidential PII.

38. By obtaining, collecting, and storing Plaintiff's and Class Members' PII, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiff's and Class Members' PII from disclosure.

39. Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality of their PII. Plaintiff and Class Members, as current and former customers, relied on Defendant to keep their PII confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

Securing PII and Preventing Breaches

40. Defendant could have reasonably prevented this Data Breach by properly securing

Plaintiff's and Class Members' PII. Additionally, Defendant could have destroyed data, including old data that Defendant had no legal right or responsibility to retain.

41. Defendant's negligence in failing to safeguard its current and former customers' PII is exacerbated by the repeated warnings and alerts that Defendant received placing it on notice of the urgent need to protect and secure sensitive data, especially sensitive financial data.

42. Despite the prevalence of public announcements of data breach and data security compromises, Defendant failed to take appropriate steps to protect the PII of Plaintiff and Class Members from being compromised.

43. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."²⁰ The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."²¹

44. The ramifications of Defendant's failure to keep secure its current and former customers' PII are long lasting and severe. Once Social Security numbers and other PII have been stolen, fraudulent use of that information and resulting damage to victims may continue for years.

Value of Personal Identifiable Information

45. The PII of individuals is of high value to criminals, as evidenced by the prices

²⁰ 17 C.F.R. § 248.201 (2013).

²¹ *Id.*

they will pay for it on the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from \$40 to \$200, and bank details command a price range of \$50 to \$200.²² Experian reports that a stolen credit or debit card number can sell for \$5 to \$110 on the dark web.²³ Criminals also can purchase access to entire sets of information obtained from company data breaches—such as the hack at issue in this case—from \$900 to \$4,500.²⁴

46. Social Security numbers are among the most sensitive kind of personal information to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. The Social Security Administration stresses that the loss of an individual's Social Security number, as is the case here, can lead to identity theft and extensive financial fraud:

A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.²⁵

²² *Your personal data is for sale on the dark web. Here's how much it costs*, Digital Trends, Oct. 16, 2019, available at: <https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/>.

²³ *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, available at: <https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/>.

²⁴ *In the Dark*, VPNOverview, 2019, available at: <https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/>.

²⁵ Social Security Administration, *Identity Theft and Your Social Security Number*, available at: <https://www.ssa.gov/pubs/EN-05-10064.pdf>.

47. What is more, it is no easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against potential misuse of a Social Security number is not permitted; an individual instead must show evidence of actual, ongoing fraud to obtain a new number.

48. Even then, a new Social Security number may not be effective. According to Julie Ferguson of the Identity Theft Resource Center, “The credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number.”²⁶

49. Thus, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach because, in that situation, victims can simply cancel or close credit and debit card accounts. By contrast, the information compromised in this Data Breach is impossible to “close” and difficult, if not impossible, to change: name, birthdate, financial history, and Social Security number.

50. This data, moreover, commands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, “Compared to credit card information, personally identifiable information and Social Security numbers are worth more than 10x on the black market.”²⁷

²⁶ Bryan Naylor, *Victims of Social Security Number Theft Find It’s Hard to Bounce Back*, NPR (Feb. 9, 2015), available at: <http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millionsworrying-about-identity-theft>.

²⁷ Time Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, (Feb. 6, 2015), available at: <https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html>.

51. Among other forms of fraud, identity thieves may obtain driver's licenses, government benefits, medical services, and housing or even give false information to police.

52. The PII of Plaintiff and Class Members was taken by hackers to engage in identity theft and/or to sell it to other criminals who will purchase the PII for that improper purpose. The fraudulent activity resulting from the Data Breach may not come to light for years.

53. Further, there may be a time lag between when harm occurs and when it is discovered, as well as between when PII is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

[L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.²⁸

54. At all relevant times, Defendant knew, or reasonably should have known, of the critical importance of safeguarding Defendant's current and former customers' PII, including Social Security numbers and financial account information, and of the foreseeable consequences that would occur if Defendant's electronic systems were breached, including, specifically, the significant costs that would be imposed on Defendant's current and former customers as a result of such an intrusion.

55. Plaintiff and Class Members now face years of needing to continuously monitor their financial and personal records. The Class is incurring and will continue to incur such damage, including valuable lost time, in addition to any fraudulent use of their PII.

²⁸ *Report to Congressional Requesters*, GAO, at 29 (June 2007), available at: <http://www.gao.gov/new.items/d07737.pdf>.

56. Defendant was, or should have been, fully aware of the unique type and the significant volume of data on Defendant's network that included millions of individuals' detailed and confidential personal information and, thus, the very large number of individuals who would be harmed by the exposure of the sensitive data.

57. Although Defendant has offered its current and former customers identity monitoring services for a limited time through Experian, the services offered are inadequate to protect Plaintiff and Class Members from the threats they face for years to come, particularly in light of the PII that Defendant negligently allowed to be taken by nefarious actors.

58. The injuries to Plaintiff and Class Members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the PII of its current and former customers.

Plaintiff Lana Clark's Experience

59. Plaintiff Clark applied for an automobile loan with TMX's subsidiary, TitleMax. As a condition to receiving services from TitleMax, Plaintiff provided her PII as part of her loan application.

60. Plaintiff Clark greatly values her privacy and PII, especially when receiving loan and financial services. Prior to the Data Breach, she took reasonable steps to maintain the confidentiality of her PII.

61. Plaintiff Clark received a letter dated March 30, 2023, from Defendant concerning the Data Breach. The letter stated that unauthorized actors gained access to TMX's network containing her name, date of birth, driver's license number, Social Security number and/or financial account information, and other information such as phone number, address, and email address.

62. Recognizing the present, immediate, and substantially increased risk of harm Plaintiff Clark faces, Defendant offered her a one-year subscription to a credit monitoring service.

63. Plaintiff Clark has been notified that her email address was discovered on the dark web and has experienced an increase in phishing emails. She has also received emails indicating that fraudulent charges may have been made on her accounts. Since learning of the Data Breach, Plaintiff Clark also has spent time researching the Data Breach and steps she can take to protect herself.

64. The Data Breach has caused Plaintiff Clark to suffer fear, anxiety, and stress.

65. Plaintiff Clark plans on taking additional time-consuming, necessary steps to help mitigate the harm caused by the Data Breach, including continually reviewing her depository, credit, and other accounts for any unauthorized activity.

66. Plaintiff Clark, like all the other Class Members, has a strong and continuing interest in ensuring that her PII, which remains in Defendant's possession, is secured against future breaches.

V. CLASS ALLEGATIONS

67. Plaintiff brings this case as a class action on behalf of herself, a Nationwide Class (the "Nationwide Class"), and a California Subclass (the "California Subclass") under Fed. R. Civ. P. 23(a), 23(b)(1), 23(b)(2), 23(b)(3), 23(c)(4) and/or 23(c)(5):

Nationwide Class. All individuals in the United States whose PII was accessed or exfiltrated during the Data Breach of TMX Finance Corporate Services, Inc., in 2022-2023.

California Subclass. All individuals in the California whose PII was accessed or exfiltrated during the Data Breach of TMX Finance Corporate Services, Inc., in 2022-2023

68. Excluded from the Class and Subclasses are the following individuals and/or entities: Defendant and its parents, subsidiaries, affiliates, officers and directors, and any entity in which it has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; any and all federal, state or local governments, including but not limited to their departments, agencies, divisions, bureaus, boards, sections, groups, counsels and/or subdivisions; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members and staff.

69. Plaintiff reserves the right to modify or amend the class definition before the Court determines whether certification is appropriate.

70. Numerosity. Consistent with Fed. R. Civ. P. 23(a)(1), the Class Members are so numerous that their joinder is impracticable. While the exact number of Class Members is unknown, upon information and belief, the Class includes approximately 4.8 million people. The number and identities of Class Members can be readily ascertained using Defendant's records.

71. Commonality. Consistent with Fed. R. Civ. P. 23(a)(2) and (b)(3), questions of law and fact common to the Class exist and predominate over any questions affecting only individual Class Members. These include:

- a. Whether Defendant failed to adequately safeguard the PII of Plaintiff and Class Members;
- b. Whether and to what extent Defendant had a duty to protect the PII of Plaintiff and Class Members;
- c. Whether Defendant had duties not to disclose the PII of Plaintiff and Class Members, respectively, to unauthorized third parties;
- d. Whether Defendant had a duty not to use the PII of Plaintiff and Class

Members for non-business purposes;

e. When Defendant learned of the Data Breach;

f. Whether Defendant adequately, promptly, and accurately informed Plaintiff and Class Members that their PII had been compromised;

g. Whether Defendant committed violations by failing to promptly notify Plaintiff and Class Members that their PII had been compromised;

h. Whether Defendant failed to implement and maintain reasonable security procedures and practices adequate to protect the information compromised in the Data Breach, considering its nature and scope;

i. Whether Defendant has adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

j. Whether Defendant engaged in unfair, unlawful, or deceptive practices, including by failing to safeguard the PII of Plaintiff and Class Members;

k. Whether Plaintiff and Class Members are entitled to actual, consequential, and/or nominal damages or restitution as a result of Defendant's wrongful conduct, and if so, in what amount; and

l. Whether Plaintiff and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm that they confront as a result of the Data Breach.

72. Typicality. Consistent with Fed. R. Civ. P. 23(a)(3), Plaintiff's claims are typical of those of other Class Members because they all had their PII compromised as a result of the Data Breach, due to Defendant's misfeasance, and their claims arise under the same legal doctrines.

73. Adequacy of Representation. Consistent with Fed. R. Civ. P. 23(a)(4), Plaintiff will fairly and adequately represent and protect the interests of the Class. Plaintiff has no interest and seeks no relief that is antagonistic or adverse to any other Class Member. She has retained counsel experienced in complex class action litigation, including data privacy cases, who intend to prosecute this action vigorously.

74. Superiority and Manageability. Consistent with Fed. R. Civ. P. 23(b)(3), class treatment is superior to all other available methods for the fair and efficient adjudication of this controversy. A class action will permit a large number of Class Members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Moreover, class action treatment will permit the adjudication of relatively modest claims by Class Members who could not individually afford to litigate a complex claim against a large corporation such as Defendant. Prosecuting the claims pleaded herein as a class action will eliminate the possibility of repetitive litigation. There will be no material difficulty in the management of this action as a class action.

75. Generally Applicable Conduct. As provided under Fed. R. Civ. P. 23(b)(2), Defendant has acted or refused to act on grounds generally applicable to the Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct in relation to the Class and making final injunctive and corresponding declaratory relief appropriate with respect to the Class as a whole. Defendant's policies challenged herein apply to and affect Class Members uniformly, and Plaintiff challenges these policies by reference to Defendant's conduct with respect to the Class as a whole.

76. Particular issues, such as questions related to Defendant's liability, also are

appropriate for certification under Fed. R. Civ. P. 23(c)(4) because the resolution of such common issues will materially advance the resolution of this matter and the parties' interests therein.

77. Class certification is also appropriate under Fed. R. Civ. P. 23(b)(1), in that the prosecution of separate actions by the individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Defendant. Prosecution of separate actions by Class Members also would create the risk of adjudications with respect to individual Class Members that, as a practical matter, would be dispositive of the interests of other members not parties to this action, or that would substantially impair or impede their ability to protect their interests.

COUNT I
Negligence
(On Behalf of Plaintiff and the Class)

78. Plaintiff re-alleges and incorporates paragraphs 1-77 as if fully set forth herein.

79. As a condition of applying for and receiving their loans from Defendant and its subsidiaries, Defendant's current and former customers were obligated to provide and entrust Defendant with certain PII, including their name, birthdate, address, Social Security number, and information provided in connection with a loan application, loan modification, or other items regarding loan servicing.

80. Plaintiff and the Class entrusted their PII to Defendant on the premise and with the understanding that Defendant would safeguard their information, use their PII for business purposes only, and/or not disclose their PII to unauthorized third parties.

81. Defendant has full knowledge of the sensitivity of the PII and the types of harm that Plaintiff and the Class could and would suffer if the PII were wrongfully disclosed or obtained by unauthorized parties.

82. Defendant knew or reasonably should have known that the failure to exercise due care in the collecting, storing, and using of its current and former customers' PII involved an unreasonable risk of harm to Plaintiff and the Class, including harm that foreseeably could occur through the criminal acts of a third party.

83. Defendant had a duty to exercise reasonable care in safeguarding, securing, and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties. This duty includes, among other things, designing, maintaining, and testing Defendant's security protocols to ensure that Plaintiff's and Class Members' information in Defendant's possession was adequately secured and protected.

84. Defendant had a duty to have procedures in place to detect and prevent the improper access and misuse of Plaintiff's and the Class's PII, and to employ proper procedures to prevent the unauthorized dissemination of the PII of Plaintiff and the Class.

85. Defendant's duty to use reasonable security measures arose as a result of the special relationship that existed between Defendant and Plaintiff and the Class. That special relationship arose because Plaintiff and the Class entrusted Defendant with their confidential PII, a mandatory step in obtaining services from Defendant.

86. Defendant was subject to an "independent duty," untethered to any contract between Defendant and Plaintiff and the Class, to maintain adequate data security.

87. A breach of security, unauthorized access, and resulting injury to Plaintiff and the Class was reasonably foreseeable, particularly in light of Defendant's inadequate security

practices and the sensitive personal information that it housed.

88. Plaintiff and the Class were the foreseeable and probable victims of inadequate security practices and procedures. Defendant knew or should have known of the inherent risks in collecting and storing the PII of Plaintiff and the Class, and the critical importance of adequately safeguarding that PII.

89. Defendant's conduct created a foreseeable risk of harm to Plaintiff and the Class. Defendant's wrongful conduct included, but was not limited to, its failure to take the steps and opportunities to prevent the Data Breach as set forth herein. Defendant's misconduct also included its failure to comply with industry standards for the safekeeping of Plaintiff's and the Class's PII.

90. Plaintiff and the Class had no ability to protect their PII to the extent it was in, and remains in, Defendant's possession.

91. Defendant was in a position to effectively protect against the harm that Plaintiff and the Class sustained as a result of the Data Breach.

92. Further, Defendant had and continues to have a duty to adequately disclose that the PII of Plaintiff and the Class within Defendant's possession was compromised, how it was compromised, and precisely the types of data that were compromised and when. Such notice was necessary to allow Plaintiff and the Class to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their PII by third parties.

93. Defendant has admitted that the PII of Plaintiff and the Class was wrongfully accessed by unauthorized third persons in the Data Breach.

94. Defendant, through its actions and inaction, unlawfully breached its duties to Plaintiff and the Class by failing to implement standard protocols and exercise reasonable care in

protecting and safeguarding the PII of Plaintiff and the Class when the PII was within Defendant's possession or control.

95. Defendant improperly and inadequately safeguarded the PII of Plaintiff and the Class in deviation of standard industry rules, regulations, and practices at the time of the Data Breach.

96. Defendant failed to heed industry warnings and alerts to provide adequate safeguards to protect its current and former customers' PII in the face of increased risk of theft.

97. Defendant, through its actions and/or omissions, unlawfully breached its duties to Plaintiff and the Class by failing to ensure appropriate procedures were in place to detect and prevent dissemination of its current and former customers' PII.

98. Defendant, through its actions and/or omissions, unlawfully breached its duties to adequately and timely disclose to Plaintiff and the Class the existence and scope of the Data Breach.

99. But for Defendant's wrongful and negligent breach of duties owed to Plaintiff and the Class, the PII of Plaintiff and the Class would not have been compromised.

100. There is a close causal connection between (a) Defendant's failure to implement security measures to protect the PII of Plaintiff and the Class and (b) the harm or risk of imminent harm suffered by Plaintiff and the Class. Plaintiff's and the Class's PII was accessed and exfiltrated as the direct and proximate result of Defendant's failure to exercise reasonable care in safeguarding such PII by adopting, implementing, and maintaining appropriate security measures.

101. Additionally, Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or

practice of businesses, such as Defendant, of failing to implement reasonable measures to protect PII. The FTC Act and related authorities form part of the basis of Defendant's duty in this regard.

102. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with applicable industry standards, as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of PII it obtained and stored and the foreseeable consequences of the damages that would result to Plaintiff and the Class.

103. Defendant's violation of Section 5 of the FTC Act constitutes negligence *per se*.

104. Plaintiff and the Class are within the class of persons that the FTC Act was intended to protect.

105. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses, which, due to their failure to employ reasonable data security measures and to avoid unfair and deceptive practices, caused the same or similar harm as that suffered by Plaintiff and the Class.

106. As a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiff and the Class have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity of how their PII is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the present and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud

and other identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their PII, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the current and former customers' PII in its continued possession; and (viii) present and future costs in the form of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the compromise of PII as a result of the Data Breach for the remainder of the lives of Plaintiff and the Class Members.

107. As a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiff and the Class have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

108. Additionally, as a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiff and the Class have suffered and will suffer the continued risks of exposure of their PII, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII in its continued possession.

109. As a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiff and the Class are now at an increased risk of identity theft or fraud.

110. As a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiff and the Class are entitled to and demand actual, consequential, and nominal damages and injunctive relief to be determined at trial.

COUNT II
Invasion of Privacy
(On Behalf of Plaintiff and the Class)

111. Plaintiff re-alleges and incorporate paragraphs 1-77 as if fully set forth herein.

112. Plaintiff and Class Members reasonably expected that the personal information they entrusted to Defendant, such as their names, Social Security numbers, addresses, and dates of birth, would be kept private and secure, and would not be disclosed to any unauthorized third party or for any improper purpose.

113. Defendant unlawfully invaded Plaintiff's and Class Members' privacy rights by:

- a. failing to adequately secure their personal information from disclosure to unauthorized third parties or for improper purposes;
- b. enabling the disclosure of personal and sensitive facts about them in a manner highly offensive to a reasonable person; and
- c. enabling the disclosure of personal and sensitive facts about them without their informed, voluntary, affirmative, and clear consent.

114. A reasonable person would find it highly offensive that Defendant, having received, collected, and stored Plaintiff's and Class Members' full names, dates of birth, and Social Security numbers and other highly sensitive personal details, failed to protect that information from unauthorized disclosure to third parties.

115. In failing to adequately protect Plaintiff's and Class Members' personal information, Defendant acted knowingly and in reckless disregard of their privacy rights. Defendant knew or should have known that its ineffective security measures, and their foreseeable consequences, are highly offensive to a reasonable person in Plaintiff's position.

116. The acts complained of herein are ongoing and/or have a substantial likelihood of being repeated.

117. Defendant's unlawful invasions of privacy damaged Plaintiff and Class Members. As a direct and proximate result of Defendant's unlawful invasions of privacy, Plaintiff and

Class Members suffered mental distress, and their reasonable expectations of privacy were frustrated and defeated. Accordingly, Plaintiff and Class Members are entitled to damages in an amount to be determined at trial.

COUNT III
Breach of Fiduciary Duty
(On Behalf of Plaintiff and the Class)

118. Plaintiff re-alleges and incorporates paragraphs 1-77 as if fully set forth herein.

119. A relationship existed between Plaintiff, the Class Members and TMX in which Plaintiff and Class Members put their trust in TMX to protect their private information and TMX accepted that trust.

120. TMX breached the fiduciary duty it owed to Plaintiff and Class Members by failing to act with the utmost good faith, fairness, and honesty, failing to act with the highest loyalty, and failing to protect the private information of Plaintiff and Class Members.

121. TMX's breach of fiduciary duty was a legal cause of damage to Plaintiff and Class Members.

122. But for TMX's breach of fiduciary duty, the damage to Plaintiff and Class Members would not have occurred.

123. TMX's breach of fiduciary duty contributed substantially to producing the damage to Plaintiff and Class Members.

124. As a direct and proximate result of TMX's breach of fiduciary duty, Plaintiff is entitled to and demand actual, consequential, and nominal damages and injunctive relief.

COUNT IV

**Violation of the California Consumer Privacy Act of 2018
Civ. Code § 1798.100, *et seq.* (“CCPA”)
(On Behalf of Plaintiff Clark and the California Subclass)**

125. Plaintiff Clark re-alleges and incorporates paragraphs 1-77 as if fully set forth herein.

126. Section 1798.150(a)(1) of the California Civil Code provides, “[a]ny consumer whose nonencrypted or nonredacted personal information, as defined by [Civil Code section 1798.81.5(d)(1)(A)] is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business’ violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information may institute a civil action for” statutory or actual damages, injunctive or declaratory relief, and any other relief the court deems proper.

127. Plaintiff Clark is a consumer and California resident as defined by Civil Code section 1798.140(i).

128. Defendant TMX is a “business” as defined by Civil Code section 1798.140(d) because it is a “sole proprietorship, partnership, limited liability company, corporation association, or other legal entity that is organized or operated for the profit or financial benefit of its shareholders or other owners that collects consumers’ personal information or on the behalf of which that information is collected and that alone, or jointly with others, determines the purposes and means of the processing of consumers’ personal information, that does business in the State of California.” TMX collects personal information from, among other sources, consumers who use its services to purchase consumer credit products. TMX has annual gross revenues in excess of \$25 million. TMX annually buys, receives for the business’s commercial purposes, sells, or

shares for commercial purposes, alone or in combination, the personal information of 100,000 or more consumers, householders, or devices.

129. Plaintiff Clark's and the California Subclass' personal information, as defined by Civil Code section 1798.81.5(d)(1)(A), was subject to unauthorized access and exfiltration, theft or disclosure. The Data Breach described herein exposed, without limitation, names, dates of birth, passport numbers, driver's license numbers, federal/state identification card numbers, tax identification numbers, Social Security numbers and/or financial account information, and other information such as phone numbers, addresses, and email addresses.

130. TMX maintained Plaintiff Clark's and the California Subclass' PII in a form that allowed criminals to access it.

131. TMX violated section 1798.150(a) of the CCPA, Cal. Civ. Code § 1798.150(a), by failing to prevent Plaintiff Clark's and the California Subclass' PII from unauthorized access and exfiltration, theft, or disclosure as a result of TMX's violations of their duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the PII.

132. As a result of the failure to implement reasonable security procedures and practices, Plaintiff Clark's and the California Subclass' PII was subjected to unauthorized access and exfiltration, theft, or disclosure as a direct and proximate result of TMX's violations of its duty under the CCPA.

133. As a consequence of TMX's violations, Plaintiff Clark and the California Subclass are entitled to all actual and compensatory damages according to proof or statutory damages allowable under the CCPA, whichever are higher, and to such other and further relief as this Court may deem just and proper, including injunctive or declaratory relief.

134. Consistent with Civil Code section 1798.150(b), Plaintiff Clark provided written notice to TMX identifying the CCPA provisions that TMX violated. If TMX is unable to cure or does not cure the violation within 30 days, Plaintiff will amend this complaint to pursue actual or statutory damages as permitted by Civil Code section 1798.150(a)(1)(A).

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of herself and the Class, prays for judgment against Defendant and respectfully requests that the Court grant the following:

- A. An Order certifying the Class and Subclasses as defined herein, and appointing Plaintiff and her counsel to represent the Class and Subclasses;
- B. Equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and the Class Members' PII, and from refusing to issue prompt, complete, and accurate disclosures to Plaintiff and the Class Members;
- C. Injunctive relief sought by Plaintiff, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and Class Members, including but not limited to an order:
 - i. prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;
 - ii. requiring Defendant to protect, including through encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state or local laws;
 - iii. requiring Defendant to delete, destroy, and purge the personally identifying information of Plaintiff and Class Members unless Defendant can provide to

the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and Class Members;

- iv. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the personally identifying information of Plaintiff and Class Members;
- v. prohibiting Defendant from maintaining Plaintiff's and Class Members' personally identifying information on a cloud-based database;
- vi. requiring Defendant to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;
- vii. requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring;
- viii. requiring Defendant to audit, test, and train its security personnel regarding any new or modified procedures;
- ix. requiring Defendant to segment data by, among other things, creating firewalls and access controls so that if one area of Defendant's network is compromised, hackers cannot gain access to other areas of Defendant's systems;
- x. requiring Defendant to conduct regular database scanning and securing checks;
- xi. requiring Defendant to establish an information security training program that

includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personally identifying information, as well as protecting the personally identifying information of Plaintiff and Class Members;

- xii. requiring Defendant to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;
- xiii. requiring Defendant to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendant's policies, programs, and systems for protecting personally identifying information;
- xiv. requiring Defendant to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendant's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;
- xv. requiring Defendant to adequately educate all Class Members about the threats that they face as a result of the loss of their confidential personally identifying information to third parties, as well as the steps affected individuals must take to protect themselves;

- xvi. requiring Defendant to implement logging and monitoring programs sufficient to track traffic to and from Defendant's servers; and, for a period of 10 years, appointing a qualified and independent third party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendant's compliance with the terms of the Court's final judgment, to provide such report to the Court and to Class Counsel, and to report any material deficiencies or noncompliance with the Court's final judgment;
- D. An award of damages, including actual, consequential, and nominal damages, or restitution in an amount to be determined;
- E. An award of reasonable attorneys' fees, costs, and litigation expenses, as allowed by law;
- F. Prejudgment interest on all amounts awarded; and
- G. Such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiff hereby demands that this matter be tried before a jury.

Date: June 21, 2023

Respectfully submitted,

By: /s/ Kris K. Skaar

Kris K. Skaar (Ga. Bar No. 649610)

Justin T. Holcombe (Ga. Bar No. 552100)

SKAAR & FEAGLE, LLP

133 Mirramont Lake Drive

Woodstock, GA 30189

Telephone: (770) 427-5600

Facsimile: (404) 601-1855

kskaar@skaarandfeagle.com

jholcombe@skaarandfeagle.com

SIGNATURES CONTINUED ON FOLLOWING PAGE

Adam E. Polk (*Pro Hac Vice Forthcoming*)
Jordan Elias (*Pro Hac Vice Forthcoming*)
Simon Grille (*Pro Hac Vice Forthcoming*)
Reid Gaa (*Pro Hac Vice Forthcoming*)

GIRARD SHARP LLP

601 California St, Ste 1400

San Francisco, CA 94108

Telephone: (415) 981-4800

apolk@girardsharp.com

jelias@girardsharp.com

sgrille@girardsharp.com

rgaa@girardsharp.com

Attorneys for Plaintiff